

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-224053

(43) 公開日 平成9年(1997)8月26日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 12/66		9466-5K	H 0 4 L 11/20	B
G 0 6 F 13/00	3 5 1		G 0 6 F 13/00	3 5 1 Z

審査請求 未請求 請求項の数 8 F D (全 17 頁)

(21) 出願番号 特願平8-147881

(22) 出願日 平成8年(1996)5月20日

(31) 優先権主張番号 4 4 4 3 5 1

(32) 優先日 1995年5月18日

(33) 優先権主張国 米国 (US)

(71) 出願人 591064003

サン・マイクロシステムズ・インコーポレーテッド

SUN MICROSYSTEMS, INCORPORATED

アメリカ合衆国 94043 カリフォルニア州・マウンテンビュー・ガルシア アヴェニュー・2550

(72) 発明者 ジェフリー・ジイ・ベール

アメリカ合衆国 94025 カリフォルニア州・メンロパーク・ケンブリッジ アヴェニュー・628

(74) 代理人 弁理士 山川 政樹

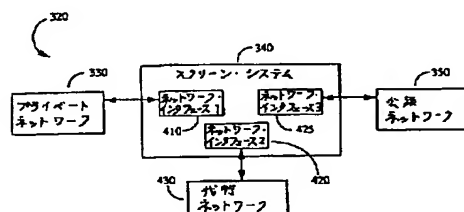
最終頁に続く

(54) 【発明の名称】 コンピュータ・ネットワーク・インタフェースにおけるデータ・パケットのパケット・フィルタリング・システム

(57) 【要約】

【課題】 プライベート・ネットワークなどの保護するネットワークと公衆ネットワークなどの他のネットワークとの間で伝送されるデータ・パケットをスクリーニングするシステムを提供する。

【解決手段】 このシステムは、プライベート・ネットワークおよび公衆ネットワークのそれぞれに接続され、プライベート・ネットワーク上にあるホストおよびサービスのサブセットをミラーリングすることができる所定の数のホストおよびサービスを含む代行ネットワークに接続された複数（特に3つ）のタイプのネットワーク・ポートを有する専用コンピュータを備える。代行ネットワークはプライベート・ネットワークから分離されており、したがって侵入者の出発点として使用することができない。



【特許請求の範囲】

【請求項 1】 第 1 のコンピュータ・ネットワークと第 2 のコンピュータ・ネットワークの間に接続されたスクリーン・システムに着信したデータ・パケットをスクリーニングし、スクリーン・システムに接続された代行システムで処置を実行する方法であって、

(1) 第 1 のネットワークから第 2 のネットワークに向けて送られた第 1 の前記パケットを現行パケットとして受信するステップと、

(2) 現行パケットの内容から現行パケットが第 2 のネットワークに渡すことを許可される所定のタイプのパケットであるか否かを判断するステップと、

(3) ステップ (2) の判断が肯定の場合、現行パケットによって指定された第 2 のネットワーク内の宛先アドレスを判断し、現行パケットを前記宛先アドレスの代わりとなる代行システム内の代用アドレスに渡すステップと、

(4) 現行パケットによって要求された少なくとも 1 つの処置が許可するようにあらかじめ決められたタイプであるか否かを判断し、そうでない場合には現行パケットを拒否してステップ (6) に進み、そうである場合にはステップ (5) に進むステップと、

(5) 現行パケットによって指定された処置をスクリーン・システムと代行システムのうちの少なくとも 1 つにおいて行うステップと、

(6) 他のパケットがスクリーン・システムに着信したか否かを判断し、着信した場合にはそのパケットを現行パケットとして受け取ってステップ (1) に進み、着信していない場合にはこの方法を終了するステップを含む方法。

【請求項 2】 ステップ (5) において、前記宛先アドレスの少なくとも一部を処置の実行場所の唯一の識別子として使用して、代行システムから第 1 のネットワークに伝送データ・パケットを伝送するステップを含む請求項 1 に記載の方法。

【請求項 3】 第 1 のコンピュータ・ネットワークと第 2 のコンピュータ・ネットワークに接続され、第 1 と第 2 のネットワークの間で伝送されるデータ・パケットをスクリーニングするスクリーン・システムであって、プロセッサと、

プロセッサに結合されたメモリと、

前記第 1 と第 2 のネットワークの間でそれぞれデータ・パケットの送信および受信を行う入力回路および出力回路と、

第 1 と第 2 ネットワークの間のデータ・パケットの流れを制御する前記メモリに記憶されたプログラム命令を含むシステムであって、

前記プログラム命令は、

第 1 のネットワークから第 2 のネットワークに伝送される第 1 のデータ・パケットが所定の基準を満たしている

か否かを判断する第 1 のプログラム・モジュールと、所定の基準を満たしている場合には第 1 のデータ・パケットを第 2 のネットワークに渡す第 2 のプログラム・モジュールと、

所定の基準を満たしていない場合には第 1 のデータ・パケットを第 2 のネットワークまで通過させないようにする第 3 のプログラム・モジュールとを備えるシステム。

【請求項 4】 第 1 のコンピュータ・ネットワークと第 2 のコンピュータ・ネットワークに接続されたスクリーン・システムに着信したデータ・パケットをスクリーニングし、スクリーン・システムに接続された代行システムで処置を実行する方法であって、

(1) 第 1 のネットワークからの第 1 の前記パケットを第 2 のネットワークで現行パケットとして受信するステップと、

(2) 第 1 のデータ・パケットの内容から第 1 のデータ・パケットの要求された操作と送信元アドレスと宛先アドレスとを判断するステップと、

(3) 少なくとも 1 つの所定の基準に基づいて、要求された操作に回答してとる処置を判断するステップと、

(4) 代行ホストが代行システムにあり、前記宛先アドレスの代わりとなる代行ホストに現行パケットを渡すステップと、

(5) 代行システムにおいて、判断された処置をとるステップを含む方法。

【請求項 5】 少なくとも 1 つのデータ・パケットが、データ・パケットの意図された受信システムを指定する第 1 のフィールドを含み、前記意図された受信システムに対して要求された操作を指定する第 2 のフィールドをさらに含む、第 1 のコンピュータ・ネットワークと第 2 のコンピュータ・ネットワークの間に結合され、前記第 1 のネットワークから前記第 2 のネットワークに送信された前記データ・パケットをスクリーニングする代行システムであって、

プロセッサと、
前記プロセッサに接続され、前記プロセッサによって実行される操作を指定する命令モジュールを記憶するように構成されたメモリと、

第 1 のデータ・パケットの内容に関する所定の基準に基づいて、前記スクリーン・システムで受信された少なくとも前記第 1 の前記データ・パケットについてとるべき所定の 1 組の処置を指定する命令を含む前記メモリに記憶された複数の処置モジュールと、

前記第 1 のデータ・パケットの前記第 2 のコンピュータ・ネットワークへの通過をスクリーン・システムが遮断する命令を含むスクリーニング・モジュールと、

前記要求された操作の代わりに前記代行システム・プロセッサによって行われるべき前記処置のうちの 1 つを選択するように前記複数の処置モジュールを制御する操作モジュールとを備える代行システム。

3

【請求項6】 第1のコンピュータ・ネットワークと第2のコンピュータ・ネットワークの間に結合されたスクリーン・システムが攻撃目標となるのを阻止する方法であって、

データ・パケットが第1のネットワークを識別する送信元アドレスと第2のネットワークを識別する宛先アドレスとを含んでいて、スクリーン・システムが、第1のネットワークから第2のネットワークに向けて送られた少なくとも1つの前記データ・パケットを受信するステップと、

所定の基準に基づいてパケットを検査するステップと、所定の基準が満たされている場合、送信元アドレスと宛先アドレスを変更せずにパケットを第2のネットワークに渡すステップと、

所定の基準が満たされていない場合、パケットを破棄すると同時にスクリーン・システムによる第1のネットワークに対するいかなる応答も阻止するステップとを含む方法。

【請求項7】 第1のコンピュータ・ネットワークと第2のコンピュータ・ネットワークの間に結合されたスクリーン・システムが攻撃目標となるのを阻止する保護システムであって、前記スクリーン・システムが、プロセッサと、そのプロセッサに結合されてプロセッサによって実行可能な命令モジュールを記憶するメモリと、スクリーン・システムを第1のネットワークに結合する第1のネットワーク・インタフェースと、スクリーン・システムを第2のネットワークに結合する第2のネットワーク・インタフェースとを備えていて、前記命令モジュールがデータ・パケットが第1のネットワークを識別する送信元アドレスと第2のネットワークを識別する宛先アドレスとを含み、第1のネットワークから第2のネットワークに向けて送られた少なくとも1つのデータ・パケットを受け取るように構成された第1のモジュールと、所定の基準に基づいてパケットを検査するように構成された第2のモジュールと、

所定の基準が満たされている場合、送信元アドレスと宛先アドレスを変更せずに第2のネットワークにパケットを渡すように構成された第3のモジュールと、

所定の基準が満たされていない場合、パケットを破棄すると同時にスクリーン・システムによる第1のネットワークに対するいかなる応答も阻止するように構成された第4のモジュールとを備える保護システム。

【請求項8】 第1のコンピュータ・ネットワークが攻撃目標となるのを阻止するシステムであって、第1のコンピュータ・ネットワークと第2のコンピュータ・ネットワークの間に結合されたスクリーン・システムを有し、そのスクリーン・システムが、プロセッサと、スクリーン・システムを第1のネットワークに結合する第1のネットワーク・インタフェースと、スクリーン・システムを第2のネットワークに結合する第2のネ

4

ットワーク・インタフェースとを備え、さらに第3のネットワーク・インタフェースを介してスクリーン・システムに結合された代行ネットワークを備え、その代行ネットワークは第1のコンピュータ・ネットワークと共有のドメインを有するインターネットワーク・アドレスを持つ少なくとも1つの代行ホストを備え、

前記スクリーン・システムは、プロセッサによって実行可能な命令モジュールを記憶する、プロセッサに結合されたメモリをさらに備え、その命令モジュールが、

10 前記ドメインを含む宛先アドレスを含むデータ・パケットを第1のネットワーク・インタフェースを介して受信する第1のモジュールと、

前記宛先アドレスが前記代行ホストに関係する場合、前記代行ホストにデータ・パケットを渡す第2のモジュールとを含むシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、1つのコンピュータ・ネットワークから他のコンピュータ・ネットワークに送信されるデータ・パケットのスクリーニングに関する。テルネット・セッション、ftp（ファイル転送プロトコル）セッション、eメール（電子メール）など、公衆ネットワーク上のユーザがプライベート・ネットワーク上のホスト機と対話する多くの方法がある。さらに、要求者の端末を直接接続するほかに、所与のターゲット・ネットワーク上のコンピュータがそのネットワークの外部のユーザから特定の操作を実行するように要求されることがある。

【0002】

30 【従来の技術】図1に、プライベート・ネットワーク20、公衆ネットワーク30、および他のプライベート・ネットワーク40を含む従来のインターネットワーク10を図示する。プライベート・ネットワーク20および40は、ファイヤーウォールを備えていないときわめて侵入を受けやすくなる。

【0003】図3に、ネットワーク・インタフェース160および170を制御する論理（回路、または典型的には関連するメモリを有するプロセッサ）150によって制御されるルータまたはブリッジ130を介してプライベート・ネットワーク120が他のプライベート・ネットワーク140と通信することができるインターネットワーク110を図示する。ネットワーク140から、ホストに宛ててネットワーク120上のポートを指定するデータ・パケットが着信すると、そのデータ・パケットはユニット180によってそのホストおよびポートに対応づけられ、インタフェース160を介してネットワーク120上の該当する宛先に送信される。図3では、セキュリティは設けられておらず、したがっていつでも攻撃目標とされる可能性がある。

50 【0004】したがって、公衆ネットワーク80を介し

てプライベート・ネットワーク60と100が互いに通信することができるがそれぞれファイアウォール70および90を備える、図2に示すシステム50におけるようなコンピュータ・ファイアウォールが開発されている。現在使用されている従来のコンピュータ・ファイアウォール（および図3のブリッジ130のようなルータまたはブリッジ）の問題点は、ファイアウォールがIP（インターネット・プロトコル）トランザクションに関与し、その際にそれらをIP機として識別する情報を発生し、それによってそれらが侵入者に認識されて攻撃目標となる点である。ファイアウォールに関するこのタイプおよびその他のタイプの問題の詳細な説明については、たとえば、参照により本明細書に組み込まれるCheswickとBellovinによる参考資料Firewalls and Internet Security (Addison Wesley 1994)とSiyanおよびHareによるInternet Firewalls and Network Security (New Riders Publishing 1995)を参照されたい。

【0005】ファイアウォールおよびパケット・フィルタリング・システムは、攻撃するために用いることができる方法の数を最小限にするように、侵入者にとって認識不能であって、それにもかかわらず適切な機能を満たすのが理想的である。

【0006】現在のネットワーク・セキュリティ解決策は、ファイアウォールを設けるほかにネットワークに変更を加える必要があり、複雑で費用が高くつくことがある。ネットワークを実質的に変更することなくネットワークに接続可能であって、保護ネットワークの外部からの侵入に対してはセキュリティを実現するシステムが必要である。

【0007】通例ルータとして機能し、保護ネットワークに結合された1つのポートまたはネットワーク・インタフェース及び他のネットワークまたはインターネットに結合された他のポートを有するパケット・フィルタリング・システムが、ネットワークにセキュリティを与えるために現在使用されている。ルータとして、このようなシステムはIPコマンドに応答し、特にそれらのシステムのIPアドレスを使用してデータ・パケットに

【0008】

【発明が解決しようとする課題】保護ネットワーク内のアドレスがそのネットワークの外部のユーザに知られた場合にも、同じタイプの攻撃を受ける。したがって、ネットワーク内のフィルタリング・システムに関するIPアドレス情報もホストに関するIPアドレス情報も明らかにせずにネットワークの外部からのデータ・パケットに

る。

【0009】

【課題を解決するための手段】本発明は、従来の意味でのファイアウォールとシグネチャレス・パケット・フィルタリング・システムの両方の機能を果たすスクリーン・システムに向けられている。たとえば公衆ネットワークと攻撃目標になることから保護するプライベート・ネットワークとの間のネットワーク接続部にスクリーンを設置する。その2つのネットワークのそれぞれについてポートまたはネットワーク・インタフェースを設け、さらに、1つまたは複数の代行ネットワークに対して1つまたは複数の追加的ポートを設ける。

【0010】このスクリーン・システムは、各着信パケットを検査してエンジンに送るパケット・フィルタリング・サブシステムまたはモジュールを備え、エンジンはパケット検査機構およびその他の情報に基づいて、そのパケットに対してどのような処置をとるべきかを決定する。パケットは処置サブシステムまたはモジュールに渡され、その処置サブシステムまたはモジュールが適切な処置を実行する。

【0011】パケットの意図された宛先がプライベート・ネットワーク上のホスト機である場合は、代わりに代行ネットワーク上の事前構成済みホスト機にそらして送ることができ、そのホスト機が、実ホストが実行するはずの適切な操作を実行するか、または所望により異なる操作を実行する。代行ホストは、実ホストのIPアドレスを使用して応答を生成するため、代行ネットワークの存在は検知することができない。このスクリーン・システムはルータではなく、したがってそれ自身のIPアドレスは持たないため、スクリーン・システムもこのようにして検出することができず、trace_route、ping、fingerなどの操作の対象とならない。

【0012】このスクリーン・システムは、プライベート・ネットワークまたは公衆ネットワークの変更を必要とせず、ネットワーク接続でインライン接続することができ、所望の数のホストによって代行ネットワークをセット・アップすることができ、それによってプライベート・ネットワークの再構成またはネットワーク・ソフトウェアの変更を行わずにセキュリティが設けられる。

【0013】このスクリーン・システムは、すべて所定の基準に照らして、エラー・メッセージ付きまたはエラー・メッセージなしでパケットを除去する、パケットを記録する、パケットまたはそのヘッダを変更するなど、パケットに対して広範囲なその他の処置を実行するように事前構成することができる。以上のおよびその他の処置はスクリーン・システムを匿名のままで実行できる。

【0014】

【発明の実施の形態】

本発明のハードウェア

図4に、本発明の実施に適したインターネットワーク・システムを示す。公衆ネットワーク200（またはインターネットなど、ネットワークのネットワーク）は、たとえばエンジニアリング・ドメイン・ネットワーク220および会社ドメイン・ネットワーク230などを含むプライベート・ネットワークまたはインターネットワーク210と通信することができる。図のようにネットワーク220とネットワーク230および200との間に従来のファイヤウォール240を配置する。ファイヤウォールは図のように、所与のプライベート・ネットワーク（220）と公衆ネットワーク（200）との間のほか、プライベート・ネットワーク200とそのプライベート・ネットワーク自体のプライベート・インターネットワーク上の他のネットワーク（210など）との間にも設置することができることに留意されたい。ネットワーク化ハードウェアおよびソフトウェアは、イーサネットなど任意の適合する従来のネットワーク化システムとすることができる。

【0015】ファイヤウォール240は、実施者の所望により、単一の機械として構成することも、一方が着信データ・パケットを処理し他方がネットワーク220からの送出データ・パケットを処理する別々の機械として構成することもできる。さらに、会社ドメイン・ネットワーク230専用の他のファイヤウォールが通常は使用されることになるが、この図には図示していない。

【0016】ネットワーク200または230から送信されたデータ・パケットは、接続300または280を介してファイヤウォール240に送られる。このファイヤウォール240は、以下に記載する点以外は従来通りとすることができる。ファイヤウォール240は、許可されたデータ・パケットを接続250を介してネットワーク220に渡す。

【0017】同様に、ネットワーク220からネットワーク200内またはネットワーク230の宛先に宛てられたデータ・パケットは、接続270を介してファイヤウォール240に送られ、ファイヤウォール240は要求に応じて、セキュリティ条件を条件として接続310（ネットワーク200宛ての場合）または接続290（ネットワーク230宛ての場合）を介して渡す。接続250および270〜310はすべて、たとえばケーブル、光ファイバ、または同様のものなど、従来のネットワーク接続とすることができる。

【0018】図5は、インターネットワーク・システム320で実施することができる本発明のパケット・スクリーン・システム340の論理ブロック図である。別法として、このインターネットワーク・システム320は図4に示すようなインターネットワークでもよく、したがってファイヤウォール240は、従来のファイヤウォール機能のすべてに加えて以下に述べるスクリーニング機能を扱うように構成されたスクリーン・システム34

0に置き換えることができる。

【0019】図5には、標準ネットワーク・インタフェース410を介してパケット・スクリーン・システム（または単に「スクリーン」）340に結合された単一のプライベート・ネットワーク330が図示されている。さらに、他の標準ネットワーク・インタフェース425を介して公衆ネットワーク350がスクリーン340に結合されている。第3のネットワークである代行ネットワーク430が、ネットワーク・インタフェース420を介してスクリーン340に結合されている。

【0020】図4および図5に示すようなファイヤウォール接続を使用して、任意の数Nのプライベート・ネットワーク（この場合は代行ネットワークを含むものとみなすことができる）を本発明の複数のスクリーン340を介して相互に結合することができ、任意の所望の数Mの公衆ネットワークに接続することができる。したがって、 $N \times M$ のスクリーン・システムを形成することができ、図5の例では $N=2$ で $M=1$ である。以下の図8Aの説明も参照されたい。

【0021】 $N=M=1$ で、データ・パケットを一方向または双方向にIPアドレスの変更なしで通過させるか、または何らかの変更を加えるが、スクリーン・システム自体のIPアドレスまたはその他のネットワーク・アドレスを追加しない、代行ネットワークのない本発明のシステムも同様に構築することが可能である。このようなシステムについては図8Bに関して後述する。

【0022】図6にユニプロセッサ・ベースまたはマルチプロセッサ・ベースのシステムとすることができるスクリーン340を詳細に示す。この実施形態では、本発明によって実行される動作を実行するために必要な命令を記憶する1つまたは複数の従来のメモリ（たとえばRAM、ROM、EPROM、ディスク記憶装置など）400に結合された単一プロセッサ390が図示されている。ネットワーク・インタフェース410〜425はプロセッサ390によって従来の方式で制御される。

【0023】プライベート・ネットワークは、典型的には多くの異なるホストを含む。例としては、eメール・ホスト360、ftp接続を管理するftp（ファイル転送プロトコル）ホスト370、およびWWW（ワールドワイド・ウェブ）サーバなどのその他サービスのためのホスト380、rlogin（リモート・ログイン）、およびrshellのためのホストなどがある。

【0024】代行ネットワーク430は代行（または仮想）ホスト435を含む。代行ホスト435は別個のコンピュータ・システムであることが好ましい。好ましい実施形態では、代行ネットワーク430は、プライベート・ネットワーク330にあるホストのサブセット（またはすべて）のそれぞれを、後述のようにしてミラーリング（すなわちその代行として機能する）仮想ホストを備える。

10

20

30

40

50

【0025】この実施形態では、二重化したい各実ホストについて1つずつの仮想（代行）ホスト、すなわち、代行メール・サーバ440、代行ftpサーバ450、およびその他の仮想ホスト460を含む上記のような仮想ホストが示されている。二重化する各実ホストには、実ホストのうちの一部または全部を含めることができる。代行ホストは、実際のターゲット・ホスト360～380ではなくそれらのホストの動作を模倣するという意味で「仮想」である。しかし、代行ホストは代行ネットワークにおいては実際のハードウェアまたはソフトウェアあるいはその両方である。

【0026】代行ネットワークに固有のホストも含めることができる。たとえば、代行ネットワーク430は、代行サーバに固有の、すなわち、単なるネットワーク330内のWWWサーバのミラーまたは代行ではないWWWサーバ445を含むことができる。この場合、ネットワーク350からユーザが、http://www.<private.network>.comへの接続を要求すると、そのユーザはWWWサーバ445に接続される。代行ネットワーク430に固有の他のサーバ455も設けることができる。

【0027】したがって、代行ネットワークは、実ホストを表す代行ホスト、または固有サーバを有する代行ホスト、あるいはその両方を、任意の組合せ（それぞれゼロから数個まで）で含むことができる。いずれの構成を採用する場合も、プライベート・ネットワーク330と代行ネットワーク430が合わさって単一の論理ネットワークまたは見かけのネットワーク345、すなわち、公衆ネットワーク350上のユーザなど部外者の視点から見て単一の見かけのドメインを形成し、ユーザがプライベート・ネットワークのサービスまたはホストにアクセスしようと試みた場合、その要求を代行ネットワークの方にそらしてミラリング代行ホストまたは固有代行ホストに送ることができ、その際そのユーザにはこれが行われたということをまったく示さない。「代行ホスト」とは、実ホストの代行を意味することも、固有ホストであるにもかかわらず代行ネットワーク上のホストであることを意味する場合もあることに留意されたい。

【0028】図7に、本発明のシステムの代替実施形態、すなわち、代行ネットワーク430全体がスクリーン340のメモリ400に記憶されているプログラム命令で実施されるか、または1つまたは複数のメモリに記憶されているプログラム命令によって制御される追加のプロセッサおよびメモリとして実施されているシステム325を示す。この場合、図6に示すスクリーン340と代行ネットワーク430は、別々の論理実体を構成するが、別々の物理実体ではない（ただし、命令、データ、コマンド、信号など自体は別々の物理実体ではある）。つまり、スクリーン340と代行ネットワークは単一のユニットであることができる。この実施形態では、代行ホスト360～380はプログラム命令によ

てエミュレートされ、いずれの実ホストの動作も、仮想代行ホスト・モジュールによって模倣することができる。本開示の残りの部分では図5～図6を参照するが、図7の実施形態にも同様に適用されるものと理解されたい。

【0029】図8Aは、図5～図6に示すスクリーン340を詳細に示した、本発明のシステムを実施するハードウェアのブロック図である。図中の同様の番号が付いた要素は同様のものである。したがって、図8Aにはさらに従来のディスク記憶装置500と、スマート・カード、キーボード、マウス、モニタ、その他の標準I/O装置などのI/O（入出力）装置510、ならびに所望のその他の従来の記憶装置またはメモリ520が追加されて備えている様子が図示されているのがわかるであろう。メモリ400に記憶されている命令またはプログラム・モジュールが、スクリーン340の動作を制御する。

【0030】1つの実施形態では、スクリーンは従来のユーザ・レベルのアクセスを行えない、すなわち、標準キーボードやモニタを備えない。これは、スクリーンの構成に改変が加えられるのを防止するセキュリティ機能である。このような実施形態では、スクリーンは、認証され、暗号化され、専用の特殊目的管理プロトコルに従った通信に対してのみ応答する、秘密IP（またはその他のプロトコル）アドレスを持つ専用ネットワーク・ポートを介して遠隔管理される。このようなプロトコルと、使用する暗号化方式、および認証方式は、スクリーン管理者が開発または選定、あるいはその両方を行う。

【0031】図8Aに示すように、スクリーン340は、公衆ネットワークに接続された（図5のような）単一ポート425の代わりに、複数ポート427を備える複数の公衆ネットワークにそれぞれ接続することができ、他のプライベート・ネットワーク335に接続された1つまたは複数の追加ポート415を備えることもできる。たとえば、プライベート・ネットワーク335を1つの会社内のエンジニアリング・ドメインeng.sun.comとすることができ、プライベート・ネットワーク330を同じ会社内の会社ドメインcorp.sun.comとすることができ、eng.sun.comドメインとcorp.sun.comドメインは、接続337を介して相互に（所望の場合は、図示されていない追加の本発明のスクリーンをまたは従来のファイアウォールを通して）通信することができ、単一のプライベート・インターネットワーク355を形成すると同時に、これらのドメインは両方ともスクリーン340によって公衆ネットワーク350からの侵入から保護される。この実施形態の代行ネットワーク430は、eng.sun.comドメインとcorp.sun.comドメインの両方の代行を備える。

【0032】したがって、本明細書の説明の以下で述べ

る通信は、単一の公衆ネットワーク350と単一のプライベート・ネットワーク330の間で行われるものと仮定するが、本発明の特徴は、スクリーン340を介して複数の公衆ネットワーク350に接続された複数のプライベート・ネットワーク330、335にも等しく適用可能である。

【0033】図8Bに示すシステム530では、プライベート・ネットワーク540は本発明にクリーン・システム540が設けられているが、代行ネットワークはない。この実施形態および他の実施形態では、データ・パケットはいずれの方向にも、それぞれのIPアドレスの変更なしで、あるいは何らかの変更は行われるがスクリーン・システム自体のIPアドレスまたはその他のネットワーク・アドレスを追加せずに送信される。アドレスを変更するか否かの決定は、所定の基準に従ってパケットごとに行うことができる。

【0034】したがって、本発明のシステム(5~9の実施形態のいずれをも含む)では、パケットとともに提供される送信元アドレスと宛先アドレスは、(変更されるか否かを問わず)そのパケットに関連する唯一のホスト識別子またはアドレスのままとする。この実施形態の代替案では、スクリーン・システムは送信元アドレスまたは宛先アドレス(あるいはその両方)の代わりに他のネットワーク・アドレスを用いることができ、その場合、新たに代用されたアドレスは、偽であるかまたはスクリーン・システム以外のホストのものである。いずれの場合も、データ・パケットには、スクリーン・システムに関係するネットワーク・アドレスは付加されない。

【0035】前述のように、スクリーン・システムはIPアドレスまたはその他のネットワーク・アドレスすらも持たないことが好ましく、IPプロトコルを「解釈」することはできるが、IP要求にตอบสนองしないように構成される。

【0036】以下に、図5~図6のシステムの動作について図9~図11に関連して詳述するが、本発明の他の実施形態にも適用されるものと理解されたい。上記および以下で述べている本発明のシステムによって実行される動作、処置、または機能のそれぞれは、プログラム命令またはモジュール、ハードウェア(たとえばASICまたはその他の回路、ROMなど)、またはそれらの何らかの組合せとして実施することができる。

【0037】データ・パケットの一般的処理

図6で、公衆ネットワーク350からホストまたはサーバ360~380のうちの1つに宛てられたデータ・パケットが着信すると、スクリーン340によってインタセプトされる。このようなパケットは一般に送信元アドレス、宛先アドレス、要求操作またはサービスあるいはその両方、およびメッセージ(電子メールの場合)、操作対象データなどのその他の情報が含まれている。

【0038】スクリーン340は、着信(および送出)

データ・パケットに対して取る処置の制御を司る命令をメモリ400に記憶している。これらの命令は、データ・パケットの前記の内容(送信元アドレスおよび宛先アドレス、サービスのタイプ、またはデータ・パケットから入手可能なその他の情報)と、パケットの送信時刻またはスクリーンによる受信時刻、公衆ネットワークとプライベート・ネットワークの間の接続状態(またはプライベート・ネットワーク内の特定のホストまたはサービスとの接続状態)、および送信元アドレスが予期された(インター)ネットワーク場所から出たものであるかなどにより間接的に入手可能な情報などその他の情報とに基づく所定の1組の基準を含む。これは、送信元ホストが予期されたドメイン内にあるか否かを判断することによって行うか、またはパケットがそのパケットのために予期されていたネットワーク・インタフェースに着信したか否かを判断することによって行うことができる。たとえば、送信元アドレスがプライベート・ネットワーク330上のホストであると識別されたパケットは、公衆ネットワーク350用のネットワーク・インタフェース425(図6)に着信してはならない。着信する場合は、侵入者がトラステッド・ホストを装ってそのプライベート・ネットワークに侵入しようとしている可能性があるという標識である。その場合、スクリーン340は応答せずにパケットを除去しなければならない。

【0039】このようなスクリーニング基準は、データ・パケットの内容の検査、外部データ(接続状況および時刻など)の参照、および所定のテーブルまたは基準を実現するのに有用なその他の情報の参照によって実現することができ、メモリ400に記憶することができる。たとえば、使用が許可されている操作およびサービスのタイプと関連するネットワーク330と通信することが許可されているすべての送信元アドレス、接続またはパケットの受け渡し許可された時刻、送信元のために予期されている場所(予期されていない送信元からの接続はセキュリティ問題を示している可能性があるため)、送信元がトランザクションの開始を許可されている回数、特定の送信元がネットワーク330のサービスの使用を許可されている(たとえば1日または1月当たりの)合計時間などのテーブルを設けることができる。

【0040】このスクリーニング基準の適用によって、スクリーン340は各データ・パケットに対して1つまたは複数の事前定義された処置をとることになる。以下に、これらの処置について述べる。

【0041】パケットに対してとる処置

スクリーン・システム340は、前述の基準と、特定のセキュリティ・プロトコル、およびシステム管理者によってあらかじめ決められた当該パケットのレベルに基づいて、各データ・パケットに対する処置をとる。たとえば、あらかじめ許可されていない送信元からの(またはそのような送信元への)パケットは通過させないことに

10

20

30

40

50

することができる。その場合、他の送信元からの（または他の送信元への）パケットは、それ以上の処置を行わずにスクリーン340によって除去され、その際、エラー・メッセージまたはその他の通信を送信側に戻す場合も戻さない場合もある。送信側にはパケットに何が起ったのかは示されず、「偽の」メッセージも出さない。

【0042】これによってシステムに対する攻撃が防止される。たとえば、パケットに応答する正規のIP手続きに従わずにtrace_routeパケットを受信した場合、本発明のスクリーンはそれを単に破棄するだけであり、このようにしてtrace_routeコマンドの発行者はスクリーンを検知することができない。

【0043】トポロジ隠蔽、すなわちパケットがスクリーンを通過したときのパケットのネットワーク・アドレスの変更を行って、パケットが多数の送信元から送られた場合であっても、スクリーンから出たパケットがすべて同じホストから送られたように見えるようにすることができる。これにより、部外者がプライベート・ネットワーク内のユーザID、ホスト名などを知ることによって入手することができる知識を利用しようとする試みが阻止される。

【0044】他の処置は、当然、単にパケットを通過させてその宛先に渡すことであり、その際、所定の基準に基づいて何らかの変更を行う場合も行わない場合もある。たとえば、プライベート・ネットワーク330内の所与のホストから送られたすべてのパケットがユーザIDまたはホストIDが除去されているようにし、パケットが他の何らかのIP送信元アドレスを付けて渡されるように、前もって決めることができる。

【0045】システム管理者によって定義された基準に従って、特定のデータ・パケットについて暗号化と暗号解読を自動的に行うこともできる。これに加えて、参照により本明細書に組み込まれる1994年9月15日出願のSystem for Signatureless Transmission and Reception of Data Packets Between Computer Networksという名称の出願人の同時係属の米国特許出願第08/306337号の事例で述べられているように、パケットをカプセル化し、パケットに新しいIPアドレスが入った新しいヘッダを付けることが望ましい。

【0046】パケットは、時刻、送信元および宛先のアドレス、要求された操作、各パケットに対してとられたその他の処置、当該送信元からそれまでに送られた要求の数など、システム管理者が重要であると決めた任意の情報を含めて（特に失敗した試行または要求）、通常ログ・ファイル記憶域640に記録される。

【0047】パケット数をカウントし、それによって特定の期間に処理された現在合計数を記録することもできる。

【0048】上記でアドレス書き換えについて述べた。パケットによって搬送されるデータまたはメッセージの書き換えまたはその他の方法による変更など所定の処置によって、パケットの他の内容も自動的に書き換えることができる。

【0049】パケットに関する状態情報も、処置によって判断し、所望であれば記録し、変更することができる。たとえば、所望に応じてTCP/IP（伝送制御プロトコル／インターネット・プロトコル）状況を変更して接続の確立、維持、または終了を行うことができる。一般に、スクリーンは、各パケットがどのような状態にあるかに関する情報を記憶し、どのパケットが初期要求だったか、応答はどれであるかなどに関する情報の維持を含む、その状態に応じた処置をとることができる。したがって、以前の事象を一定期間のあいだ記憶していなければならないことがあるが、その場合はスクリーンが一連のトランザクションの全履歴を判断し、その都度適切な処置をとることができる。

【0050】セキュリティのための重要な処置は、あたかも代行ホストが実際の意図された宛先サーバであるかのようにパケットに対して操作を実行する前述のようなサーバ／ホストを備えた代行ネットワーク430に、パケットをそらして送信する処置である。このような操作の実行時、代行ホストは所与のパケットを送信側に戻すこと、すなわち元の送信側アドレスを宛先としてパケットを送信することができる。そのパケットは次にスクリーン340を通り、スクリーン340は、たとえば公衆ネットワーク350から、スクリーンで最初に受け取ったときと同じように、パケットを所定の検査基準にかける。この基準は一般に、代行ネットワーク430またはプライベート・ネットワーク330から送られたパケットについて異なる結果をもたらす。たとえば、公衆ネットワークの外部のホストはプライベート・ネットワークとのテルネット・セッションを確立することができないが、プライベート・ネットワーク内のホストはプライベート・ネットワークの外部のホストとのテルネット・セッションを確立することが「できる」ものと決めることができる。

【0051】スクリーン・システムは（IPまたはその他の）ネットワーク・アドレスを持たないことによって、そのセキュリティ機能を匿名で実行することができ、特に、従来のネットワーク・ブリッジとして機能しない。スクリーン340がブリッジの機能を備えているとすれば、IPコマンドに回答しなければならないことになり、したがって検知可能となり攻撃目標となる。

【0052】代行ネットワークはさらに、部外者が決して実際にプライベート・ネットワーク330に侵入できないようにするという利点を有する。ユーザがいったんプライベート・ネットワークへのアクセスまたは接続を許可されると、アクセスがまったく許可されない場合と

比較して、そのユーザのアクションを制限することははるかに困難になる。代行ネットワーク内のプライベート・ネットワークのサービスの一部の、複製またはミラーリングされた機能、または、代行ネットワーク内の固有ホストまたはその他のサービス（ハードウェアまたはソフトウェア、あるいはその両方）の機能、あるいはその両方によって、外部ユーザの要求が満たされると同時に、そのユーザが実際にプライベート・ネットワークにアクセスするのを、見えない方式で防ぐ。

【0053】さらに、代行パケットはシステムによる「信用度」が高いため、代行ネットワークからのパケットはスクリーンによる再送信のために乗り越えなければならないハードルが一般に低くなるので、プライベート・ネットワークのセキュリティを危険にさらす可能性があるセッションを代行ネットワークからはまったく確立できないようにすることもできる。代行ネットワークがTCPセッションを開始することができるようにすると、システムの外部からの侵入者は、公衆ネットワークからセッションを開始しなくても、代行ネットワークにTCPセッションを開始させる方法を見つけ出すことができた場合、ファイアウォール・セキュリティを事実上迂回することができる。

【0054】プライベート・ネットワーク「から」公衆ネットワーク「への」特定の接続を確立することができるようにし、その逆はできないようにすることが望ましい場合がある。たとえば、公衆ネットワーク350へのTCPセッション（テルネットまたはftpなど）は、プライベート・ネットワーク330内のユーザによっては開始することができるが、公衆ネットワークからプライベート・ネットワークへは遮断される。

【0055】一般に、代行ネットワークによって行われるすべての処置は、代行ネットワークまたはその中のホストを別個のIP実体として識別することなく、パケットを受け渡す。したがって、パケットは処理後に受け渡しされるか戻されると、指定された宛先ホストによって実際に処理されたように見えるか（実際に代行ホストがそれを処理した場合）、または宛先アドレス（戻りパケットの送信元アドレス）を除去、変更またはその他の方法でわからないようにするように処理される。いずれの場合も、代行ホスト用のIPアドレスは存在せず、いかなるパケットに追加されることもない。

【0056】スクリーン・システムの機能アーキテクチャ

図9は、図8に対応する機能ブロック図であるが、スクリーン340によって使用される機能モジュールが示されている。好ましい実施形態では、これらのモジュールは、前記のように、メモリ400に記憶されていてプロセッサ390によって実行されるプログラム命令モジュールである。

【0057】図9に示すモジュールは、各ネットワーク

・インタフェース410〜425用のプロセス602〜606を有するパケット検査機能600と、規則620を有するエンジンと610と、処置630およびログ・ファイル記憶域640と、従来のハッシュ・テーブルであるパケット状態テーブル650と、キャッシュ分割モジュール670（図のような分割迂回路を有する）と、各ネットワーク・インタフェース410〜425に結合されたパケット分割機能660と、学習ブリッジ・テーブル680とを含む。図9に示す接続は、本発明の特定の物理的实施態様に応じて、論理（ソフトウェア）命令またはハードウェア命令、あるいはその両方を指す。

【0058】パケット検査機能600は、前述の基準に基づいて着信パケットの内容を検査する命令を備える。つまり、どこからであっても着信データ・パケットが送られてくると、各着信パケットはパケット検査機能600によるパケット検査を受ける。

【0059】エンジン610が着信パケットを処理して処置630に渡し、前述のようにそれらのパケットに対して適切な操作が行われる。処置モジュール630は、これらの操作の実行専用のモジュールである。

【0060】ログ・ファイル記憶域640を使用して、前述のように、スクリーン340で受信されたデータ・パケットに関する情報が記憶される。同時にパケット状態テーブル650を使用して、受信パケットの状態に関する情報が記憶される。

【0061】分割機能660は従来の方式で機能して所定の最大伝送単位（MTU）より大きいパケットを分割する。これは、たとえばスクリーンがパケットに情報を追加してその大きさがこの許容最大サイズを超える大きさにした場合に起こることがある。分割キャッシュ670を従来の方式で使用してパケットの分割と再構成を行う。一般に分割パケットは、主にまたは単にIPヘッダ情報とデータのみを含み（特に、ポート番号は含まれない）、スクリーン340は分割キャッシュを使用してパケットを必要に応じて再構築する。つまり、最初の分割パケットが分割キャッシュに記憶され、それ以降の分割パケットも同様に記憶されて、最後の分割パケットを受信してから、そのパケットが再構成される。

【0062】分割迂回路675は、分割キャッシュ670内で情報が見つかった分割パケットのエンジン操作をパケット検査機能が迂回するために使用される。したがって、一連の分割パケットの中の2番目以降の分割パケットを受信すると、そのことはパケット検査機能600が分割キャッシュ670を調べたときに検出される。その場合、新たに受信した分割パケットは、エンジン610を介さずに迂回路675を介して処置630に送られる。

【0063】学習ブリッジ・テーブル680によって、スクリーン340は従来の学習ブリッジとして機能することができる。すなわち、どのホストがスクリーンのど

10

20

30

40

50

ちら側にあるかを追跡し、スクリーンのポート（ネットワーク・インタフェース）のそれぞれに一方のホストまたは他方のホストからパケットが着信すると、この情報のテーブルのメンテナンスを行う。

【0064】スクリーン・システムの動作

図10～図11は、本発明の方法の好ましい実施形態を示すフロー・チャートである。たとえば公衆ネットワーク350のホストによってパケットが送られると、そのパケットはスクリーン340のポート（インタフェース）425で受けられる。図10のボックス800を参照されたい。パケット検査機能が前述のようにパケットの内容を検査する（ボックス810）。

【0065】パケットを拒否する場合、（送信元アドレスの）学習ブリッジ・テーブル680を使用してそれを行うと効率的である。

【0066】パケット検査を実施するのに適した1つの実施形態を、図11のフロー・チャートに示すが、多くの変更態様が可能である。この例示のフロー・チャートでは、パケットを受け取ると（ボックス900）、各パケット・ヘッダが順に検査される（ボックス910）。すなわち、物理リンク（IPなど）、IPヘッダ（TCPか否か）、TCPヘッダ（どのポートが指定されているか、および既存の接続か新規の接続かに関して）などが検査される。

【0067】ボックス920および940で、否定の判断であればボックス930に進んで適切な処置がとられる。肯定の判断であればボックス950に進み、指定されているポートが判断され、ボックス960に進み、ヘッダ情報のほか、パケットの内容、送信元、宛先、および前述のその他の情報など、パケット検査機能が自由に使える情報を考慮して、その特定の接続が許可されるか否かが判断される。

【0068】その接続が許可されない場合は遮断される（ボックス970）、許可される場合は、この方法はそれが初期接続であるか否かを調べる（ボックス980）。初期接続の場合は、ボックス990でその接続が確立され、ボックス995で状態テーブル650（図9参照）に情報が格納されて、その新しい接続が識別される。初期接続でない場合は、ボックス1010で接続が検査され、更新情報（たとえば接続に関する新しい情報）があればそれがテーブル650に格納される。

【0069】この方法は、ステップ990または1020からボックス1000に進む。すなわち図10のボックス810に戻る。

【0070】前述のように図11は、パケット検査段階で行うことができる多くの可能な検査および操作の順序の、1つの実施形態に過ぎないことが理解されよう。図11で実行される動作は、（たとえばボックス920、940、960、および980での）パケット検査の結果に基づいてエンジン600によって行われる。

【0071】図10のボックス820に進んで、パケットはエンジン610に渡され、エンジン610は前述の事前定義された適切な操作を実行する。一般に、ファイヤウォール/スクリーン340の場合、これにはパケットの遮断または通過が伴い、通過させる場合にはパケットは代行ネットワーク430内の代行ホストによって操作されるようにそらすことができる。

【0072】したがって、現行パケットは適切な処置の実行のために処置モジュール630に渡され（ボックス830）、ボックス840でエンジンは、パケット検査機能の結果とどの処置をとるのが適切であったかというエンジン自身の判断とに基づいて、とるべき処置が他にないかどうかを判断する。所与のパケットの最初の通過時には、（たとえばパケットを除去してそれ以上の処置を行わない場合などそれが「唯一の」処置である場合であっても）取るべき処置が少なくとも1つあることになり、したがって最初の通過時にはボックス840からボックス850に進み、最初の処置がとられる。

【0073】この方法は次にボックス830に戻り、このループはエンジンによって判断されたすべての処置が処置モジュールによって行われると完了する。その時点で、ボックス840の次にボックス860に進み、スクリーン340が、入力ポート（ネットワーク・インタフェース）の1つに他のパケットがあるか否かを判断する。ある場合には、この方法はボックス800で新たに開始し、ない場合にはこの方法はボックス870で終了する。新しいパケットを受信するといつでも再び開始することができる。

【図面の簡単な説明】

【図1】 2つのコンピュータ・ネットワークを公衆ネットワークを介して接続するシステムのブロック図である。

【図2】 介在ファイヤウォールを使用して、2つのコンピュータ・ネットワークを公衆ネットワークを介して接続するシステムのブロック図である。

【図3】 2つのコンピュータ・ネットワーク間にブリッジを備える従来のシステムを示す図である。

【図4】 ファイヤウォールを介した、プライベート・ネットワークおよび公衆ネットワークから他のプライベート・ネットワークへの接続例を示すブロック図である。

【図5】 本発明によるパケット・スクリーン・システムを備えるコンピュータ・インターネットワークのブロック図である。

【図6】 インターネットワーク上の本発明のパケット・スクリーン・システムを示す機能ブロック図である。

【図7】 本発明のパケット・スクリーン・システムの代替実施形態を示すブロック図である。

【図8】 本発明を実施するハードウェアのブロック図である。

19

20

【図 9】 本発明の機能ブロック図である。

【図 10】 本発明の好ましい実施形態によるパケット・スクリーニングの方法を示すフロー・チャートである。

【図 11】 本発明の好ましい実施形態によるパケット・スクリーニングの方法を示すフロー・チャートである。

【符号の説明】

320 インターネットワーク・システム

330 プライベート・ネットワーク

340 スクリーン・システム

345 論理ネットワーク

350 公衆ネットワーク

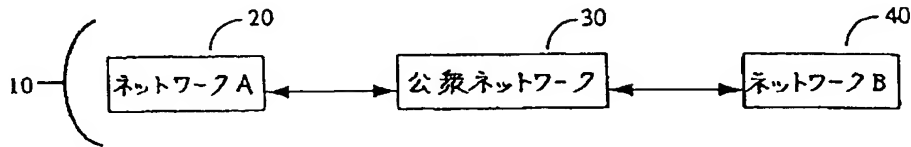
410 ネットワーク・インタフェース

420 ネットワーク・インタフェース

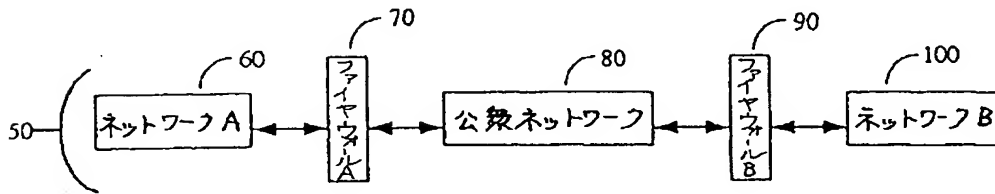
425 ネットワーク・インタフェース

430 代行ネットワーク

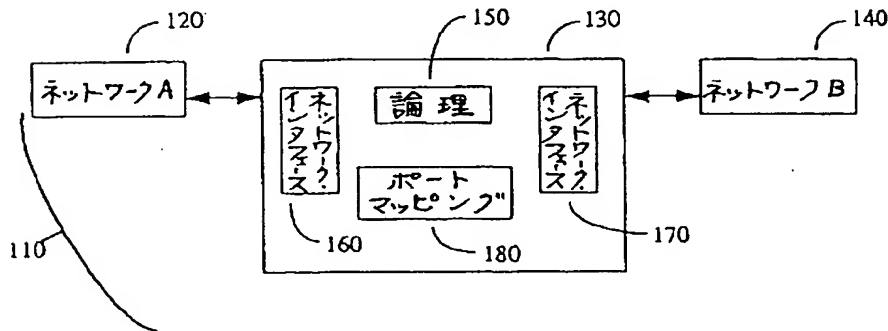
【図 1】



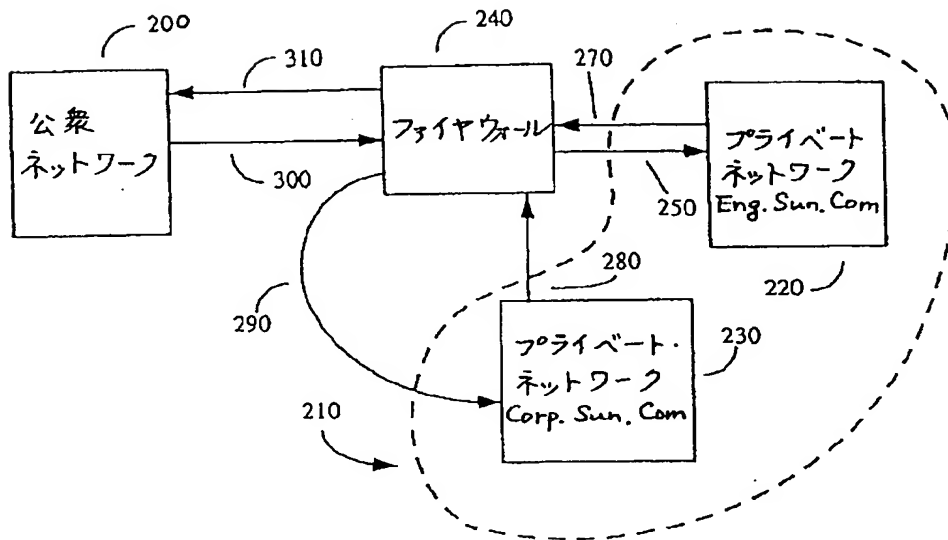
【図 2】



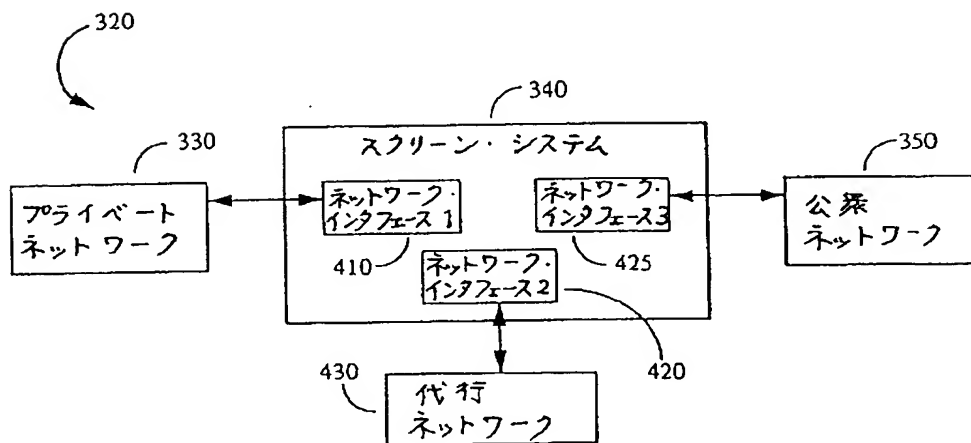
【図 3】



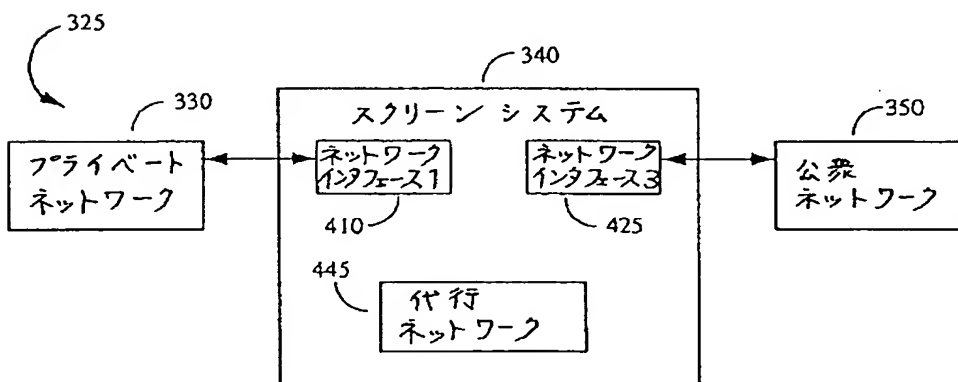
【図 4】



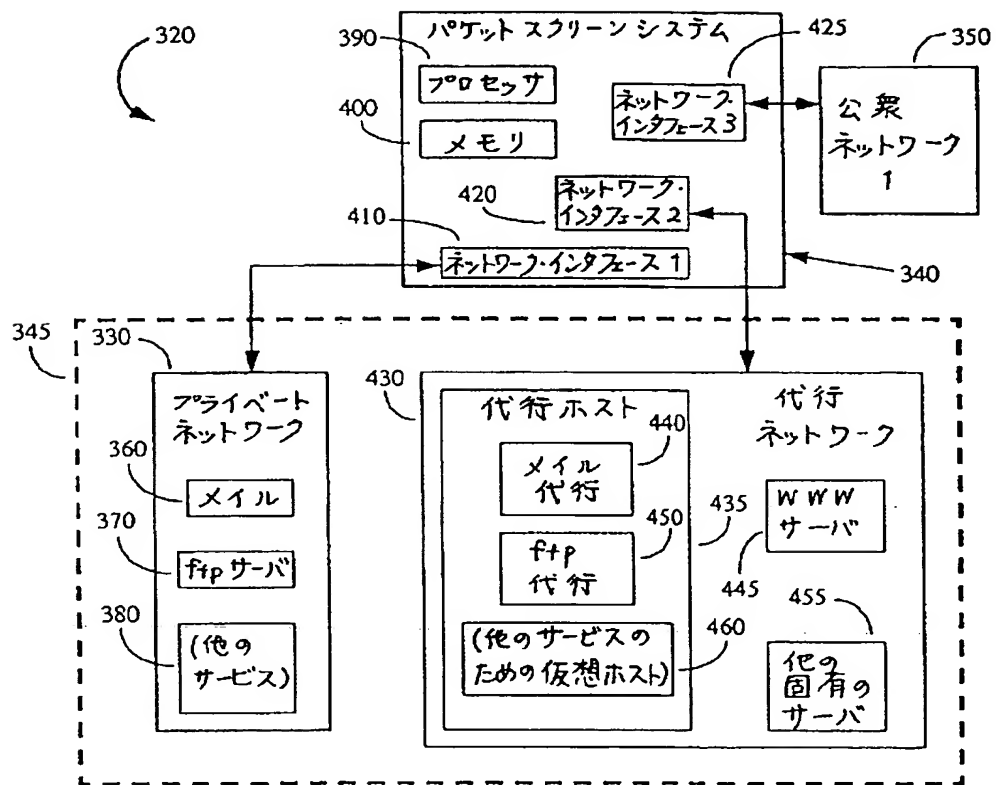
【図 5】



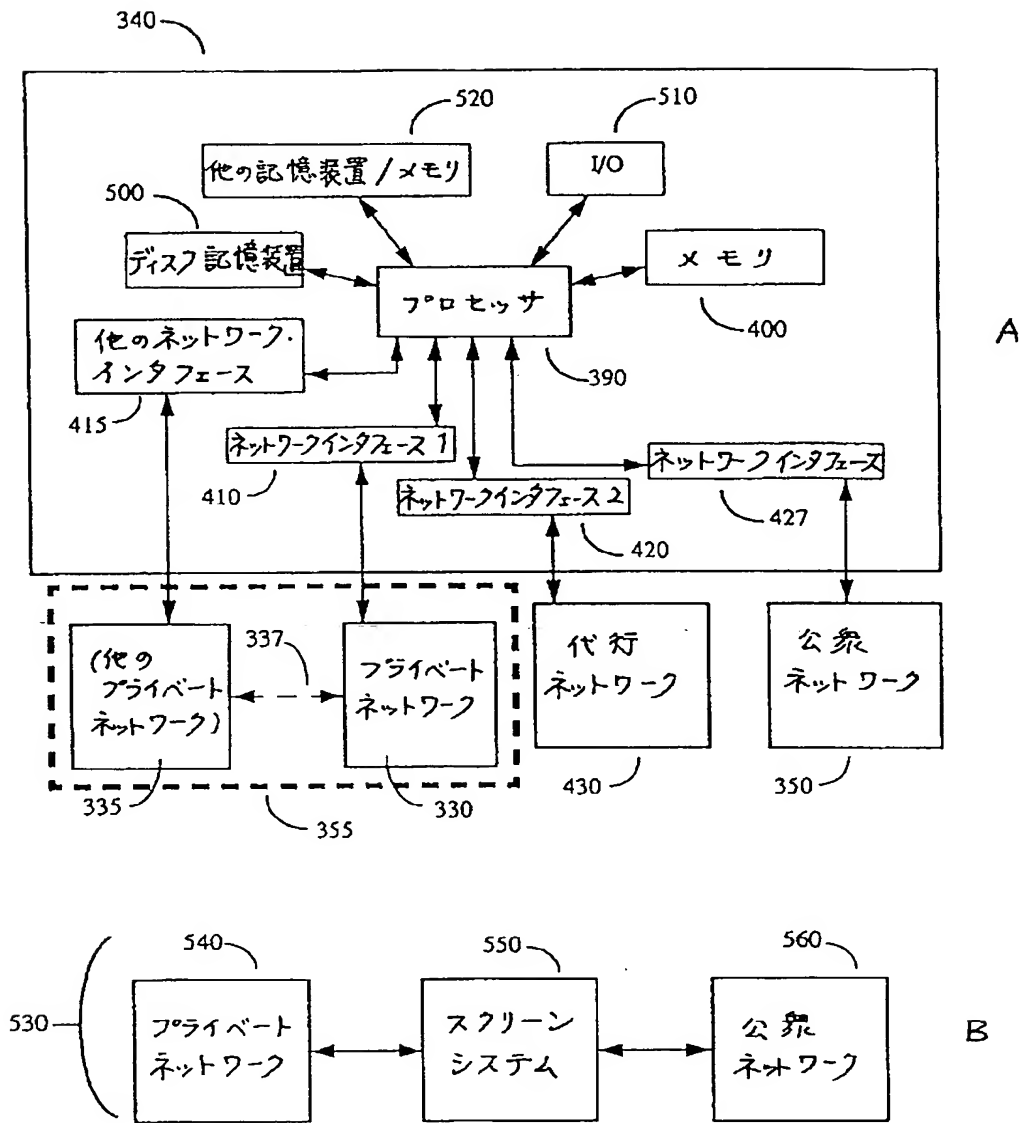
【図 7】



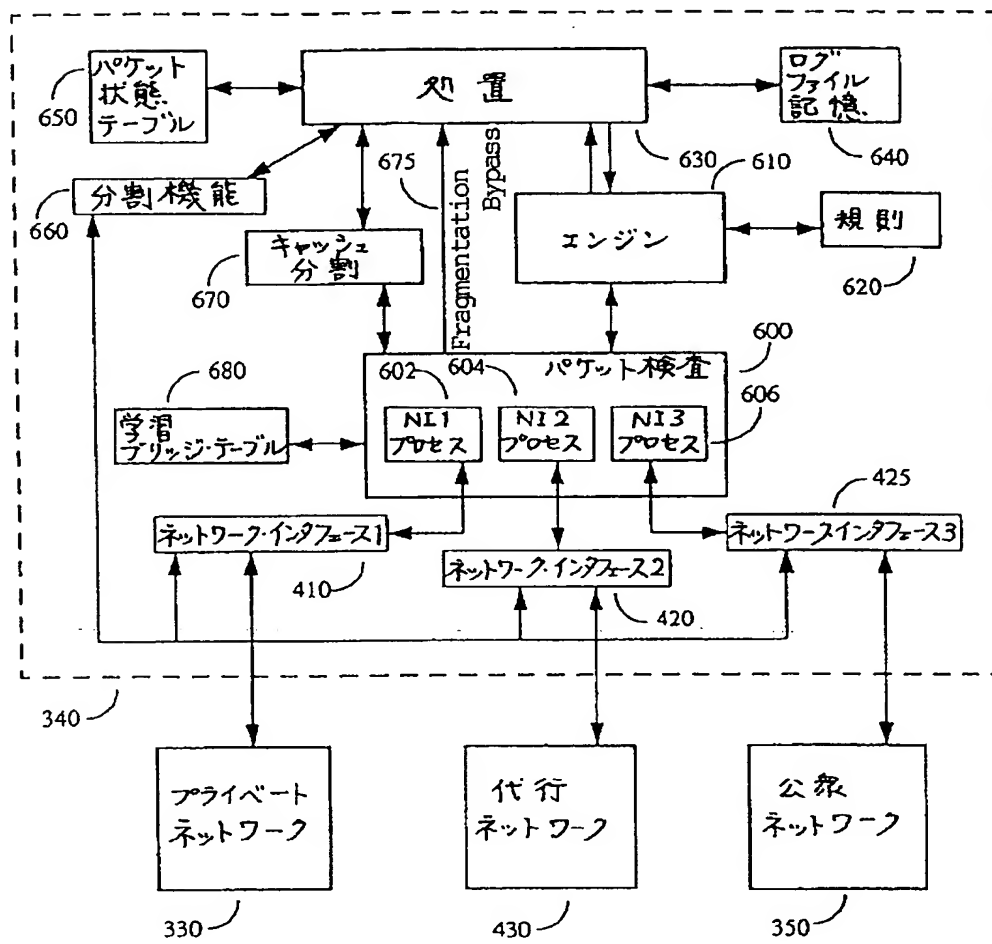
【図 6】



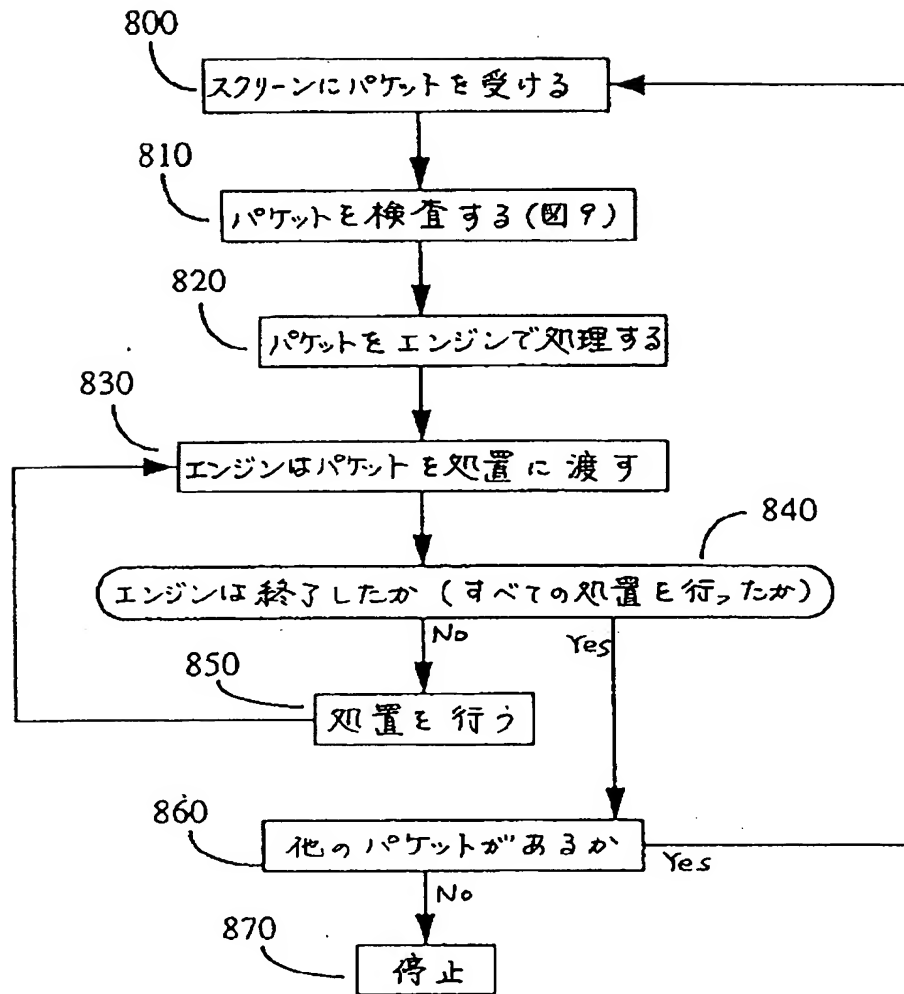
【図 8】



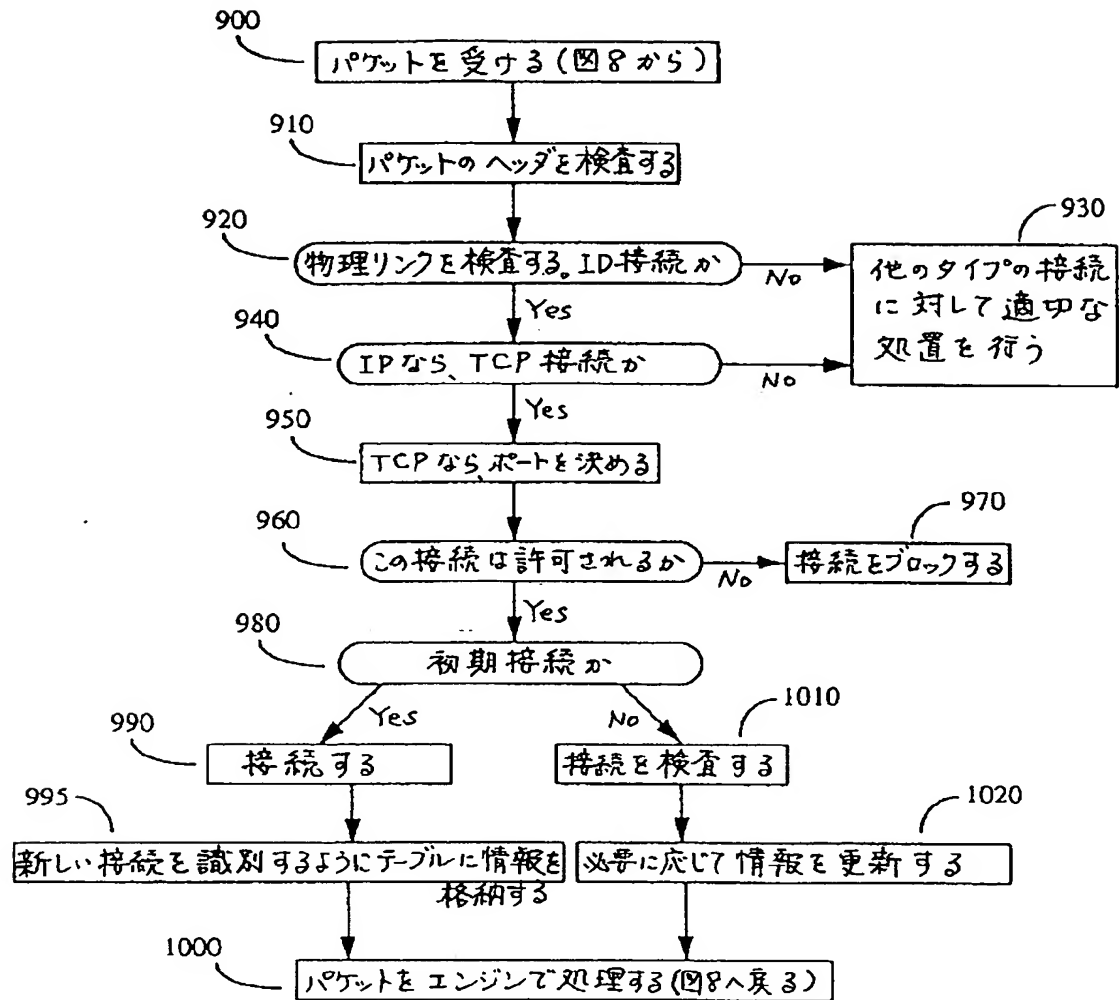
【図9】



【図10】



【図 11】



フロントページの続き

(72) 発明者 ウィリアム・ダニエルソン
アメリカ合衆国 94040 カリフォルニア
州・マウンテンビュー・カトリーナ ウェ
イ・2728

(72) 発明者 トーマス・エル・ライアン
アメリカ合衆国 94301 カリフォルニア
州・パロ アルト・エッジウッド ドライ
ブ・1400

(72) 発明者 ジェフリー・マリガン
アメリカ合衆国 94555 カリフォルニア
州・フレモント・ウィンプラル コート・
3330

(72) 発明者 マーティン・バターソン
フランス国 38000 グルノーブル・リュ
ドゥ ポストン・5

(72) 発明者 グレン・シイ・スコット
アメリカ合衆国 93561 カリフォルニア
州・デハチャピ・ムーン ドライブ・
19700

(72) 発明者 キャロライン・タービフィル
アメリカ合衆国 95030 カリフォルニア
州・ロス ガトス・アーモンド ヒル コ
ート・105